TINA WOLFSON (SBN 174806)
twolfson@ahdootwolfson.com
ROBERT AHDOOT (SBN 172098)
rahdoot@ahdootwolfson.com
THEODORE MAYA (SBN 223242)
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521
Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH (*pro hac vice*)
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

BEN BARNOW (*pro hac vice*)
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL (*pro hac vice*)
aparkhill@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60606
Telephone: 312.621.2000

Attorneys for Plaintiffs and the Proposed Class

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

DOUGLAS FEHLEN and TONY BLAKE, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

ACCELLION, INC.,

Defendant.

Case No. 5:21-cv-01353-EJD

Hon. Edward J. Davila

FIRST AMENDED CLASS ACTION COMPLAINT

JURY TRIAL DEMANDED

Complaint Filed March 17, 2021

Plaintiffs Douglas Fehlen and Tony Blake ("Plaintiffs"), individually and on behalf of all others similarly situated, upon personal knowledge of facts pertaining to themselves, respectively, and on information and belief as to all other matters, by and through undersigned counsel, brings this First Amended Class Action Complaint against Defendant Accellion, Inc. ("Accellion" or "Defendant").

NATURE OF THE ACTION

1. Plaintiffs bring this class action on behalf of themselves and all other individuals ("Class Members") who had their sensitive personal information—including but not limited to names, email addresses, phone numbers, home addresses, dates of birth, Social Security numbers (SSN), financial information, medical, health, and prescription information, banking information, employee information, and other sensitive information (collectively, "Personal Information")—disclosed to unauthorized third parties during a data breach compromising Accellion's legacy File Transfer Appliance software (the "Data Breach").

2. Accellion made headlines in late 2020/early 2021 (and continues to receive a raft of negative publicity) following its December 23, 2020 disclosure to numerous clients that criminals breached Accellion's client submitted data via a vulnerability in its represented "secure" file transfer application.[1]

3. Accellion is a software company that provides third-party file transfer services to clients. Accellion makes and sells a file transfer service product called the File Transfer Appliance ("FTA"). Accellion's FTA is a 20-year-old, obsolete, "legacy product" that was "nearing end-of-life"[2] at the time of the Data Breach, thus leaving it vulnerable to compromise and security incidents.

4. During the Data Breach, unauthorized persons gained access to Accellion's clients' files by exploiting a vulnerability in Accellion's FTA platform.

[1] Lucas Ropek, *The Accellion Data Breach Seems to Be Getting Bigger,* GIZMODO (Feb. 11, 2021, 8:47 P.M.), https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357.

[2] ACCELLION, *Accellion Responds to Recent FTA Security Incident* (Jan. 12, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/ (last visited July 7, 2021)

5. On February 19, 2021, The Kroger Co. ("Kroger") publicly confirmed that the Personal Information of Kroger pharmacy customers, along with "certain associates' HR data . . . and certain money services records," was compromised in the well-publicized Data Breach of its file transfer software vendor, Accellion.

6. In a press release, Kroger identified that, inter alia, customers of Kroger Health and Money Services were impacted.[3] Little information is available about the disclosure of Kroger employee and money service customer records, but reports indicate more specifically that pharmacy customers of The Little Clinic, Kroger Pharmacies, and Kroger's family of pharmacies operated by Ralphs Grocery Company and Fred Meyer Stores Inc. are all potentially impacted by the Data Breach. Other affiliated pharmacies possibly impacted by the Data Breach include Jay C Food Stores, Dillon Companies, LLC, Baker's, City Market, Gerbes, King Soopers, Quality Food Centers, Roundy's Supermarkets, Inc., Copps Food Center Pharmacy, Mariano's Metro Market, Pick 'n Save, Harris Teeter, LLC, Smith's Food and Drug, Fry's Food Stores, Healthy Options, Inc., Postal Prescription Services, and Kroger Specialty Pharmacy.[4]

7. On January 23, 2021, Accellion informed Kroger that Kroger's files and information were impacted by the Data Breach. Specifically, Accellion notified Kroger that an unauthorized person gained access to certain Kroger files by exploiting a vulnerability in Accellion's FTA platform.

8. At the time of the Data Breach, Kroger, along with reportedly numerous others, was a client of Accellion. Accellion's services to Kroger, and the other customers, included the use of Accellion's outdated and vulnerable FTA platform for large file transfers. The Personal Information of Kroger's pharmacy customers, employees, and money service customers, and customers of many other companies

---

[3] The Kroger Co., *Accellion Security Incident Impacts Kroger Family of Companies Associates and Limited Number of Customers,* CISION PR NEWSWIRE (Feb. 19, 2021, 4:05 P.M.), https://www.prnewswire.com/news-releases/accellion-security-incident-impacts-kroger-family-of-companies-associates-and-limited-number-of-customers-301231891.html.

[4] Chris Mayhew, *Kroger advises customers of a data breach affecting pharmacy and Little Clinic,* CINCINATI.COM | THE ENQUIRER (Feb. 19, 2021, 8:34 A.M.), https://www.cincinnati.com/story/news/2021/02/19/kroger-warns-customers-medical-prescriptions-data-breach/4514664001/.

who are or were clients of Accellion, was accessed by and disclosed to criminals without authorization because the criminals were able to exploit vulnerabilities in Accellion's FTA product.

9. Accellion was well aware of the data security shortcomings in its FTA product. Nevertheless, Accellion continued to use FTA with its clients, putting Accellion's file transfer service clients and their clients' customers and employees at risk of being impacted by a breach.

10. Accellion's failure to ensure that its file transfer services and products were adequately secure fell far short of its obligations and Plaintiffs' and Class Members' reasonable expectations for data privacy, has jeopardized the security of their Personal Information, and has put them at serious risk of fraud and identity theft.

11. As a result of Accellion's conduct and the Data Breach, Plaintiffs' and Class Members' privacy has been invaded. Their Personal Information is now in the hands of criminals, and they face a substantially increased risk of identity theft and fraud. Accordingly, these individuals now must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

PARTIES

12. Plaintiff Douglas Fehlen is a citizen of Washington and resides in Vancouver, Washington. He received a notice letter from Kroger stating that his Personal Information was compromised by the Data Breach. In the letter, Kroger confirmed to Plaintiff that "[this] incident involved your personal information" and that the "impacted information may include names, email address and other contact information, date of birth, Social Security number, and for some associates or former associates, may have also included certain salary information. . . . ."

13. Plaintiff Tony Blake is a citizen of North Carolina and resides in Chapel Hill, North Carolina. He received a notice letter from Kroger stating that his Personal Information was compromised by the Data Breach. In the letter, Kroger confirmed to Plaintiff that "[this] incident involved your personal information" and that the "[i]mpacted information includes all, or a subset of, the following: certain names, email address, phone numbers, home addresses, dates of birth, information to process insurance claims, prescription information such as prescription number, prescribing doctor, medication names and dates, medical history, as well as certain clinical services, such as whether you were ordered an influenza test.

14. Defendant Accellion Inc. is a Delaware corporation with corporate headquarters located at 1804 Embarcadero Road, Suite 200, Palo Alto, California 94303.

JURISDICTION AND VENUE

15. This Court has subject matter jurisdiction over this action pursuant to the Class Action Fairness Act of 2005, 28 U.S.C. § 1332(a) and (d), because the matter in controversy, exclusive of interest and costs, exceeds the sum or value of five million dollars ($5,000,000.00) and is a class action in which Plaintiffs are citizens of states different from Defendant. Further, greater than two-thirds of the Class Members reside in states other than the state in which Defendant is a citizen.

16. The Court has personal jurisdiction over Accellion because Accellion has a principal office in California, does significant business in California, and otherwise has sufficient minimum contacts with and intentionally avails itself of the markets in California through its promotion, marketing, and sale of file transfer services.

17. Venue properly lies in this judicial district because, *inter alia,* Defendant has a principal place of business, transacts substantial business, has agents, and is otherwise located in this district; and a substantial part of the conduct giving rise to the claims occurred in this judicial district.

FACTUAL ALLEGATIONS

A. Accellion and its Unsecure File Transfer Platform, FTA

18. Accellion is a Palo Alto-based software company that makes, markets, and sells file transfer platforms and services.

19. Accellion touts its products and services as "prevent[ing] data breaches"[5] and as being secure. On its website, Accellion states:

> The Accellion enterprise content firewall *prevents data breaches and compliance violations from third party cyber risk*. CIOs and CISOs *rely on the Accellion platform for complete visibility, security and control* over . . . *sensitive content* across email, file sharing, mobile, enterprise apps, web portals, SFTP, and automated inter-business workflows.[6]

[5] ACCELLION, *About Accellion,* https://www.accellion.com/company/ (last visited July 7, 2021).

[6] *Id.* (emphasis added).

20. Accellion also touts its commitment to data privacy, claiming that "[d]ata privacy is a fundamental aspect of the business of Accellion . . . ."[7]

21. Accellion markets its products and services as capable of safely transferring sensitive Personal Information through file sharing, claiming that "[w]hen employees click the Accellion button, they know it's the *safe*, *secure* way to share sensitive information. . . ."[8]

22. Despite these assurances and claims, Accellion failed to offer safe and secure file transfer products and services and failed to adequately protect Plaintiffs' and Class Members' Personal Information entrusted to it by Accellion's clients.

23. This is because the product that Accellion offered, and which its clients used, was not secure and, by Accellion's own acknowledgment, outdated.

24. The FTA—or File Transfer Appliance—is Accellion's twenty-year-old "legacy" file transfer software, which purportedly is designed and sold for large file transfers.[9]

25. According to Accellion, the product has become an obsolete "legacy product" that was "nearing end-of-life,"[10] thus leaving it vulnerable to compromise and security incidents. Accellion acknowledged that the FTA program is insufficient to keep file transfer processes secure "in today's breach-filled, over-regulated world" where "you need even broad protection and control."[11]

26. Key people within Accellion have acknowledged the need to leave the FTA platform behind due to the security concerns raised by it. Accellion's Chief Marketing Officer Joel York confirmed

---

[7] ACCELLION, *Accellion Privacy Policy*, https://www.accellion.com/privacy-policy/ (last visited July 7, 2021).

[8] ACCELLION, *About Accellion*, https://www.accellion.com/company/ (last visited July 7, 2021) (emphasis added).

[9] ACCELLION, *Accellion Responds to Recent FTA Security Incident* (Jan. 12, 2021), https://www.accellion.com/company/press-releases/accellion-responds-to-recent-fta-security-incident/.

[10] ACCELLION, *Press Release, Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/.

[11] ACCELLION, *Accellion FTA*, https://www.accellion.com/products/fta/ (last visited July 7, 2021).

that Accellion is encouraging its clients to discontinue use of FTA because it does not protect against modern data breaches: "It just wasn't designed for these types of threats . . . ."[12]

27. Accellion's Chief Information Security Officer Frank Balonis stated: "Future exploits of [FTA] . . . are a constant threat. We have encouraged all FTA customers to migrate to kiteworks for the last three years and have accelerated our FTA end-of-life plans in light of these attacks. We remain committed to assisting our FTA customers, but strongly urge them to migrate to kiteworks as soon as possible."[13]

28. Despite knowing that FTA leaves Accellion customers and third parties interacting and transacting with its customers (like Plaintiffs and other Class Members) exposed to security threats, it continued to offer and transact business with its customers using the FTA file transfer product.

B. The Accellion Data Breach

29. On December 23, 2020, the inevitable happened: Accellion confirmed to numerous clients that it experienced a massive security breach whereby criminals were able to gain access to sensitive client data via a vulnerability in its FTA platform.[14]

30. According to reports, the criminals exploited as many as four vulnerabilities in Accellion's FTA to steal sensitive data files associated with up to 300 of Accellion's clients, including corporations, law firms, banks, universities, and other entities.

31. With respect to how Accellion's FTA was compromised, one report indicates:

> The adversary exploited [the FTA's] vulnerabilities to install a hitherto unseen Web shell named DEWMODE on the Accellion FTA app and used it to exfiltrate data from victim networks. Mandiant's telemetry shows that DEWMODE is designed to extract a list of

---

[12] Jim Brunner & Paul Roberts, *Banking, Social Security info of more than 1.4 million people exposed in hack involving Washington State Auditor*, SEATTLE TIMES (Feb. 3, 2021, 4:57 P.M.), https://www.seattletimes.com/seattle-news/politics/personal-data-of-1-6-million-washington-unemployment-claimants-exposed-in-hack-of-state-auditor/.

[13] ACCELLION, *Press Release, Accellion Provides Update to Recent FTA Security Incident* (Feb. 1, 2021), https://www.accellion.com/company/press-releases/accellion-provides-update-to-recent-fta-security-incident/.

[14] Lucas Ropek, *The Accellion Data Breach Seems to Be Getting Bigger,* GIZMODO (Feb. 11, 2021), https://gizmodo.com/the-accellion-data-breach-seems-to-be-getting-bigger-1846250357.

available files and associated metadata from a MySQL database on Accellion's FTA and then download files from that list via the Web shell. Once the downloads complete, the attackers then execute a clean-up routine to erase traces of their activity.[15]

32. The criminals, reportedly associated with the well-known Clop ransomware gang, the FIN11 threat group, and potentially other threat actors, launched the attacks in mid-December 2020. The attacks continued from at least mid-December 2020 and into January 2021, as these actors continued to exploit vulnerabilities in the FTA platform. Following the attacks, the criminals resorted to extortion, threatening Accellion's clients, e.g., by email, with making the stolen information publicly available unless ransoms were paid.[16] In at least a few instances, the criminals carried these threats and published private and confidential information online.

33. An example of a message reportedly sent by the criminals to a client of Accellion that was victimized during the breach is below[17]:

> Hello!
>
> Your network has been hacked, a lot of valuable data stolen. <description of stolen data, including the total size of the compressed files> We are the CLOP ransomware team, you can google news and articles about us. We have a website where we publish news and stolen files from companies that have refused to cooperate. Here is his address http://[redacted].onion/ - use TOR browser or http://[redacted].onion.dog/ - mirror. We are visited by 20-30 thousand journalists, IT experts, hackers and competitors every day. We suggest that you contact us via chat within 24 hours to discuss the current situation. <victim-specific negotiation URL> - use TOR browser We don't want to hurt, our goal is money. We are also ready to provide any evidence of the presence of files with us.

34. Accellion has remained in the headlines through early 2021 (and continues to receive a raft of negative publicity) following its mid-December 2020 disclosure of the massive Data Breach. The list

---

[15] Jai Vljayan, *Accellion Data Breach Resulted in Extortion Attempts Against Multiple Victims,* DARKREADING (Feb. 22, 2021, 4:50 P.M.), https://www.darkreading.com/attacks-breaches/accellion-data-breach-resulted-in-extortion-attempts-against-multiple-victims/d/d-id/1340226.

[16] Ionut Ilascu, *Global Accellion data breaches linked to Clop ransomware gang,* BLEEPINGCOMPUTER (Feb. 22, 2021, 9:06 A.M.), https://www.bleepingcomputer.com/news/security/global-accellion-data-breaches-linked-to-clop-ransomware-gang/.

[17] *Id.*

of groups and clients who used Accellion's unsecure FTA product and were impacted by the Data Breach continues to increase and includes, among others:

- Allens
- American Bureau of Shipping ("ABS")
- Arizona Complete Health
- The Australia Securities and Investments Commission
- Bombardier
- CSX
- Danaher
- Flagstar Bank
- Fugro
- Goodwin Proctor
- Harvard Business School
- Jones Day
- The Kroger Co.
- The Office of the Washington State Auditor
- QIMR Berghofer Medical Research Institute
- Qualys
- The Reserve Bank of New Zealand
- Shell
- Singtel
- Southern Illinois University School of Medicine
- Stanford University
- Steris
- Transport for New South Wales
- Trillium Community Health Plan
- University of California system
- University of Colorado

- University of Maryland, Baltimore
- University of Miami (Florida)
- Yeshiva University.

C. Kroger Announces it was Impacted by the Accellion Data Breach

35. On January 23, 2021, Accellion notified Kroger that unauthorized persons gained access to Kroger's files containing Plaintiffs' and Class Members' Personal Information by exploiting multiple zero-day vulnerabilities in Accellion's FTA.

36. On February 19, 2021, Kroger publicly confirmed that the Personal Information of Kroger pharmacy customers, along with "certain associates' HR data . . . and certain money services records," was compromised in the Data Breach. Kroger specifically identified that customers of Kroger Health and Money Services were impacted.[18]

37. On its website, Kroger provides the following, in pertinent part[19]:

> **Information About the Accellion Incident**
>
> Kroger has confirmed that it was impacted by the data security incident affecting Accellion, Inc. Accellion's services were used by Kroger, as well as many other companies, for third-party secure file transfers. Accellion notified Kroger that an unauthorized person gained access to certain Kroger files by exploiting a vulnerability in Accellion's file transfer service.
>
> Here are the facts as we understand them: The incident was isolated to Accellion's services and did not affect Kroger's IT systems or any grocery store systems or data. No credit or debit card (including digital wallet) information or customer account passwords were affected by this incident. After being informed of the incident's effect on January 23, 2021, Kroger discontinued the use of Accellion's services, reported the incident to federal law enforcement, and initiated its own forensic investigation to review the potential scope and impact of the incident.
>
> * * *
>
> What information may have been involved?

[18] The Kroger Co., *Accellion Security Incident Impacts Kroger Family of Companies Associates and Limited Number of Customers,* CISON PR NEWSWIRE (Feb. 19, 2021, 4:05 P.M.), https://www.prnewswire.com/news-releases/accellion-security-incident-impacts-kroger-family-of-companies-associates-and-limited-number-of-customers-301231891.html (last visited July 7, 2021).

[19] KROGER, *Accellion Incident*, https://www.kroger.com/i/accellion-incident (last visited Feb. 22, 2021).

> At this time, based on the information provided by Accellion and our own investigation, Kroger believes the categories of affected data may include certain associates' HR data, certain pharmacy records, and certain money services records.

38. The breach was extensive insofar as its impact on Kroger's pharmacy customers, including customers of The Little Clinic, Kroger Pharmacies, and Kroger's family of pharmacies operated by Ralphs Grocery Company and Fred Meyer Stores Inc., all of which are potentially impacted by the Data Breach, potentially along with other affiliated pharmacies.[20]

D. Impact of the Data Breach

39. As a result of the FTA Data Breach, Plaintiffs and millions of individuals have had their information exposed. Many other Accellion clients have reported being impacted by the Data Breach, and potentially millions of additional persons have had their sensitive Personal Information exposed as a result of Accellion's unsecure FTA product being exploited by criminals during the Data Breach.

40. The harm caused to Plaintiffs and Class Members by the Data Breach is already apparent. As identified herein, criminal hacker groups already are threatening Accellion's clients with demands for ransom payments to prevent sensitive Personal Information from being disseminated publicly.

41. Even if companies that were impacted by the Accellion Data Breach pay these ransoms, there is no guarantee that the criminals making the ransom demands will suddenly act honorably and destroy the sensitive Personal Information. In fact, there is no motivation for them to do so, given the burgeoning market for sensitive Personal Information on the dark web.

42. The breach creates a heightened security concern for Plaintiffs and Class Members because SSNs and sensitive health and prescription information was included. Theft of SSNs creates a particularly alarming situation for victims because those numbers cannot easily be replaced. In order to obtain a new number, a breach victim has to demonstrate ongoing harm from misuse of her SSN, and a new SSN will not be provided until after the harm has already been suffered by the victim.

---

[20] Chris Mayhew, *Kroger advises customers of a data breach affecting pharmacy and Little Clinic,* CINCINATI.COM | THE ENQUIRER (Feb. 19, 2021, 8:34 A.M.), https://www.cincinnati.com/story/news/2021/02/19/kroger-warns-customers-medical-prescriptions-data-breach/4514664001/.

43. Given the highly sensitive nature of SSNs, theft of SSNs in combination with other personally identifying information (e.g., name, address, date of birth) is akin to having a master key to the gates of fraudulent activity. Per the United States Attorney General, Social Security numbers "can be an identity thief's most valuable piece of consumer information."[21]

44. Accellion had a duty to keep Personal Information confidential and to protect it from unauthorized disclosures. Plaintiffs and Class Members provided their Personal Information to Kroger with the common sense understanding any business partners to whom Kroger disclosed the Personal Information (i.e., Accellion) would comply with their obligations to keep such information confidential and secure from unauthorized disclosures.

45. Accellion's data security obligations were particularly important given the substantial increase in data breaches—particularly those involving health information— in recent years, which are widely known to the public and to anyone in Accellion's industry of data collection and transfer.

46. Data breaches are by no means new and they should not be unexpected. These types of attacks should be anticipated by companies that store sensitive and personally identifying information, and these companies must ensure that data privacy and security is adequate to protect against and prevent known attacks.

47. It is well known among companies that store sensitive personally identifying information that sensitive information—like the SSNs and prescription and other health information stolen in the Data Breach—is valuable and frequently targeted by criminals. In a recent article, *Business Insider* noted that "[d]ata breaches are on the rise for all kinds of businesses, including retailers. . . . Many of them were caused by flaws in . . . systems either online or in stores."[22]

---

[21] *Fact Sheet: The Work of the President's Identity Theft Task Force*, DEP'T OF JUSTICE, (Sept. 19, 2006), https://www.justice.gov/archive/opa/pr/2006/September/06_ag_636.html.

[22] Dennis Green, Mary Hanbury & Aine Cain, *If you bought anything from these 19 companies recently, your data may have been stolen*, BUSINESS INSIDER (Nov. 19, 2019, 8:05 A.M.), https://www.businessinsider.com/data-breaches-retailers-consumer-companies-2019-1.

48. Identity theft victims are frequently required to spend many hours and large amounts of money repairing the impact to their credit. Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, tax fraud, phone or utilities fraud, and bank/finance fraud.

49. There may be a time lag between when sensitive personal information is stolen and when it is used. According to the GAO Report:

> [L]aw enforcement officials told us that in some cases, *stolen data may be held for up to a year or more before being used to commit identity theft*. Further, once stolen data have been sold or posted on the Web, *fraudulent use of that information may continue for years*. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[23]

50. With access to an individual's Personal Information, criminals can do more than just empty a victim's bank account—they can also commit all manner of fraud, including: obtaining a driver's license or official identification card in the victim's name but with the thief's picture; using the victim's name and SSN to obtain government benefits; or, filing a fraudulent tax return using the victim's information. In addition, identity thieves may obtain a job using the victim's SSN, rent a house, or receive medical services in the victim's name, and may even give the victim's personal information to police during an arrest, resulting in an arrest warrant being issued in the victim's name.[24]

51. Personal Information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the dark web and the "cyber black-market" for years. As a result of recent large-scale data breaches, identity thieves and cyber criminals have openly posted stolen SSNs and other Personal Information directly on various illegal websites making the information publicly available, often for a price.

52. A study by Experian found that the "average total cost" of medical identity theft is "about $20,000" per incident, and that a majority of victims of medical identity theft were forced to pay out-of-pocket costs for healthcare they did not receive in order to restore coverage.[25] Indeed, data breaches and

---

[23] *Id*. at 29 (emphasis added).

[24] *See* FEDERAL TRADE COMMISSION, WARNING SIGNS OF IDENTITY THEFT, https://www.identitytheft.gov/Warning-Signs-of-Identity-Theft (last visited Feb. 22, 2021).

[25] *See* Elinor Mills, *Study: Medical identity theft is costly for victims*, CNET (Mar. 3, 2010, 5:00 A.M.), https://www.cnet.com/news/study-medical-identity-theft-is-costly-for-victims.

identity theft have a crippling effect on individuals and detrimentally impact the entire economy as a whole.

53. Medical information is especially valuable to identity thieves. According to a 2012 Nationwide Insurance report, "[a] stolen medical identity has a $50 street value – whereas a stolen social security number, on the other hand, only sells for $1."[26] In fact, the medical industry has experienced disproportionally higher instances of computer theft than any other industry.

54. Despite the known risk of data breaches and the widespread publicity and industry alerts regarding other notable (similar) data breaches, Accellion failed to take reasonable steps to adequately protect its systems from being breached and to properly phase out its unsecure FTA platform, which it knew was unsecure, leaving its clients and all persons who provide sensitive Personal Information to its clients exposed to risk of fraud and identity theft.

55. Accellion is, and at all relevant times has been, aware that the sensitive Personal Information it handles and stores in connection with providing its file transfer services is highly sensitive. As a company that provides file transfer services involving highly sensitive and identifying information, Accellion is aware of the importance of safeguarding that information and protecting its systems and products from security vulnerabilities.

56. Accellion was aware, or should have been aware, of regulatory and industry guidance regarding data security, and it was alerted to the risk associated with failing to ensure that its file transfer product FTA was adequately secured, or phasing out the platform altogether.

57. Despite the well-known risks of hackers and cybersecurity intrusions, Accellion failed to employ adequate data security measures in connection with offering its file transfer products and services in a meaningful way in order prevent breaches, including the Data Breach.

58. The security flaws inherent to Accellion's FTA file transfer platform—and continuing to market and sell a platform with known, unpatched security issues—run afoul of industry best practices

[26] Study: Few Aware of Medical Identity Theft Risk, CLAIMS JOURNAL (June 14, 2012), http://www.claimsjournal.com/news/national/2012/06/14/208510.htm.

and standards. Had Accellion adequately protected and secured FTA, or stopped supporting the product when it learned years ago about its vulnerabilities, it could have prevented the Data Breach.

59. Despite the fact that Accellion was on notice of the very real possibility of data theft associated with the FTA platform, it still failed to make necessary changes to the product or to stop offering and supporting it, and permitted a massive intrusion to occur that resulted in the FTA platform's disclosure of Plaintiffs' and Class Members' Personal Information to criminals.

60. Accellion permitted Class Members' Personal Information to be compromised and disclosed to criminals by failing to take reasonable steps against an obvious threat.

61. Industry experts are clear that a data breach is indicative of data security failures. Indeed, industry-leading research and advisory firm Aite Group has identified that: "If your data was stolen through a data breach that means you were somewhere out of compliance" with payment industry data security standards.[27]

62. As a result of the events detailed herein, Plaintiffs and Class Members suffered harm and loss of privacy, and will continue to suffer future harm, resulting from the Data Breach, including but not limited to: invasion of privacy; loss of privacy; loss of control over personal information and identities; fraud and identity theft; unreimbursed losses relating to fraud and identity theft; loss of value and loss of possession and privacy of Personal Information; harm resulting from damaged credit scores and information; loss of time and money preparing for and resolving fraud and identity theft; loss of time and money obtaining protections against future identity theft; and other harm resulting from the unauthorized use or threat of unauthorized exposure of Personal Information.

63. Victims of the Data Breach have likely already experienced harms, which is made clear by news of attempts to exploit this information for money by the hackers responsible for the breach.

64. As a result of Accellion's failure to ensure that its FTA product was protected and secured, or to phase out the platform upon learning of FTA's vulnerabilities, the Data Breach occurred. As a result of the Data Breach, Plaintiffs' and Class Members' privacy has been invaded, their Personal Information

[27] Lisa Baertlein, *Chipotle Says Hackers Hit Most Restaurants in Data Breach*, REUTERS (May 26, 2017), http://www.reuters.com/article/us-chipotle-cyber-idUSKBN18M2BY.

is now in the hands of criminals, they face a substantially increased risk of identity theft and fraud, and they must take immediate and time-consuming action to protect themselves from such identity theft and fraud.

CLASS ALLEGATIONS

65. Plaintiffs bring this action on their own behalf, and on behalf of the following Class pursuant to Federal Rule of Civil Procedure 23(a) and (b):

Nationwide Class

All residents of the United States whose Personal Information was compromised in the Accellion Data Breach occurring in December 2020 and January 2021.

66. In the alternative, Plaintiffs seek to certify the following state subclasses:

Washington Subclass

All residents of the state of Washington whose Personal Information was compromised in the Accellion Data Breach occurring in December 2020 and January 2021.

North Carolina Subclass

All residents of the state of North Carolina whose Personal Information was compromised in the Accellion Data Breach occurring in December 2020 and January 2021.

67. Excluded from the Class are Accellion and its affiliates, officers, directors, assigns, successors, and the Judge(s) assigned to this case.

68. **Numerosity**: While the precise number of Class Members has not yet been determined, members of the Class are so numerous that their individual joinder is impracticable, as the proposed Class appears to include many millions of members who are geographically dispersed.

69. **Typicality**: Plaintiffs and all Class Members were injured through Accellion's uniform misconduct and assert identical claims against Accellion. Accordingly, Plaintiffs' claims are typical of Class Members' claims.

70. **Adequacy**: Plaintiffs' interests are aligned with the Class they seek to represent and have retained counsel with significant experience prosecuting complex class action cases, including cases

involving alleged privacy and data security violations. Plaintiffs and counsel intend to prosecute this action vigorously. The Class's interests are well-represented by Plaintiffs and undersigned counsel.

71. **Superiority**: A class action is the superior—and only realistic—mechanism to fairly and efficiently adjudicate Plaintiffs' and other Class Member's claims. The injury suffered by each individual Class member is relatively small in comparison to the burden and expense of individual prosecution of complex and expensive litigation. It would be very difficult if not impossible for Class Members individually to effectively redress Accellion's wrongdoing. Even if Class Members could afford such individual litigation, the court system could not. Individualized litigation presents a potential for inconsistent or contradictory judgments. Individualized litigation increases the delay and expense to all parties, and to the court system, presented by the complex legal and factual issues of the case. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court.

72. **Commonality and Predominance:** The following questions common to all Class Members predominate over any potential questions affecting individual Class Members:

- whether Accellion engaged in the wrongful conduct alleged herein;
- whether Accellion was negligent or negligent per se;
- whether Accellion's data security practices and the vulnerabilities of its FTA product resulted in the unauthorized disclosure of Plaintiffs' and other Class Members' Personal Information;
- whether Accellion violated privacy rights and invaded Plaintiffs' and Class Members' privacy; and
- whether Plaintiffs and Class Members are entitled to damages, equitable relief, or other relief and, if so, in what amount.

73. Given that Accellion has engaged in a common course of conduct as to Plaintiffs and the Class, similar or identical injuries and common law and statutory violations are involved, and common questions outweigh any potential individual questions.

CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Nationwide Class)

74. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

75. Accellion negligently sold and continued to support its unsecure FTA product which it has acknowledged was vulnerable to security breaches, despite representing that the product could be used securely for large file transfers.

76. Accellion was entrusted with, stored, and otherwise had access to the Personal Information of Plaintiffs and Class Members.

77. Accellion knew, or should have known, of the risks inherent to storing the Personal Information of Plaintiffs and Class Members, and to not ensuring that the FTA product was secure. These risks were reasonably foreseeable to Accellion, including because it had previously recognized and acknowledged the data security concerns with its FTA product.

78. Accellion owed duties of care to Plaintiffs and Class Members whose Personal Information had been entrusted to Accellion.

79. Accellion breached its duties to Plaintiffs and Class Members by failing to provide fair, reasonable, or adequate data security. Accellion had a duty to safeguard Plaintiffs' and Class Members' Personal Information and to ensure that its systems and products adequately protected Personal Information. Accellion breached its duty.

80. Accellion's duty of care arises from its knowledge that its file transfer customers entrust to it highly sensitive Personal Information that Accellion is intended to, and represents that it will, handle securely. Only Accellion was in a position to ensure that its systems and products were sufficient to protect against breaches that exploit its FTA product and the harms that Plaintiffs and Class Members have now suffered.

81. A "special relationship" exists between Accellion, on the one hand, and Plaintiffs and Class Members, on the other hand. Accellion entered into a "special relationship" with Plaintiffs and Class Members by agreeing to accept, store, and have access to sensitive Personal Information provided by Plaintiffs and Class Members to Accellion's clients.

82. But for Accellion's wrongful and negligent breach of its duties owed to Plaintiffs and Class Members, Plaintiffs and Class Members would not have been injured.

83. Accellion acted with wanton disregard for the security of Plaintiffs' and Class Members' Personal Information, especially in light of the fact that for years Accellion warned of the data security concerns relating to the FTA.

84. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Accellion's breach of its duties. Accellion knew or should have known that it was failing to meet its duties, and that Accellion's breach would cause Plaintiffs and Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

85. Plaintiffs and Class Members suffered more than just economic harm as a result of the Data Breach. Plaintiffs and Class Members suffered loss of time, loss of value of their Personal Information, and loss of privacy concerning their Personal Information.

86. As a direct and proximate result of Accellion's negligent conduct, Plaintiffs and Class Members now face a certain increased risk of future harm. For them, the purpose for criminals to steal Personal Information is to sell it on the dark web for a profit to other criminals who purchase the information and use it to make fraudulent transactions or to support ransomware.

87. As a direct and proximate result of Accellion's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT II
Negligence Per Se
(On Behalf of Plaintiffs and the Nationwide Class)

88. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

89. Pursuant to the Federal Trade Commission Act (15 U.S.C. § 45), Accellion had a duty to provide adequate data security practices, including in connection with its sale of its FTA platform, to safeguard Plaintiffs' and Class Members' Personal Information.

90. Pursuant to HIPAA (42 U.S.C. § 1302d *et. seq*.), Accellion had a duty to implement reasonable safeguards to protect Plaintiffs' and Class Members' Personal Information.

91. Accellion breached its duties to Plaintiffs and Class Members under the Federal Trade Commission Act (15 U.S.C. § 45) and HIPAA (42 U.S.C. § 1302d *et. seq*.), among other laws, by failing

to provide fair, reasonable, or adequate data security in connection with the sale and use of the FTA platform in order to safeguard their Personal Information.

92. Accellion's failure to comply with applicable laws and regulations constitutes negligence per se.

93. But for Accellion's wrongful and negligent breach of its duties owed to Plaintiffs and other Class Members, they would not have been injured.

94. The injury and harm suffered by Plaintiffs and Class Members was the reasonably foreseeable result of Accellion's breach of its duties. Accellion knew or should have known that it was failing to meet its duties, and that Accellion's breach would cause Plaintiffs and other Class Members to experience the foreseeable harms associated with the exposure of their Personal Information.

95. As a direct and proximate result of Accellion's negligent conduct, Plaintiffs and other Class Members have suffered loss of time, loss of value of their Personal Information, and loss of privacy concerning their Personal Information, and now face an increased risk of future harm. As a direct and proximate result of Accellion's negligent conduct, Plaintiffs and Class Members have suffered injury and are entitled to damages in an amount to be proven at trial.

COUNT III
Invasion of Privacy (Intrusion Upon Seclusion)
(On Behalf of Plaintiffs and the Nationwide Class)

96. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

97. Plaintiffs and other Class Members had a reasonable expectation of privacy in the Personal Information that Accellion disclosed without authorization.

98. By failing to keep Plaintiffs' and other Class Members' Personal Information safe, knowingly utilizing and continuning support for the unsecure FTA platform, and disclosing Personal Information to unauthorized parties for unauthorized use, Accellion unlawfully invaded Plaintiffs' and Class Members' privacy by, *inter alia*:

(a) intruding into Plaintiffs' and Class Members' private affairs in a manner that would be highly offensive to a reasonable person; and

(b) invading Plaintiffs' and Class Members' privacy by improperly using their Personal Information properly obtained for a specific purpose for another purpose, or

disclosing it to some third party;

(c) failing to adequately secure their Personal Information from disclosure to unauthorized persons; and

(d) enabling the disclosure of Plaintiffs' and Class Members' Personal Information without consent.

99. Accellion knew, or acted with reckless disregard of the fact that, a reasonable person in Plaintiffs' and Class Members' position would consider its actions highly offensive.

100. Accellion knew that its FTA platform was vulnerable to exploitation and a breach prior to the Data Breach.

101. Defendant invaded Plaintiffs' and Class Members' right to privacy and intruded into Plaintiffs' and Class Members' private affairs by disclosing their Personal Information to unauthorized persons without their informed, voluntary, affirmative, and clear consent.

102. As a proximate result of such unauthorized disclosures, Plaintiffs' and Class Members' reasonable expectations of privacy in their Personal Information was unduly frustrated and thwarted. Defendant's conduct amounted to a serious invasion of Plaintiffs' and Class Members' protected privacy interests.

103. In failing to protect Plaintiffs' and Class Members' Personal Information, and in disclosing Plaintiffs' and Class Members' Personal Information, Accellion acted with malice and oppression and in conscious disregard of Plaintiffs' and Class Members' rights to have such information kept confidential and private.

104. Plaintiffs seek injunctive relief on behalf of the Class, restitution, and all other damages available under this Count.

COUNT IV
Violation of the North Carolina Unfair Deceptive Trade Practices Act
N.C. Gen. Stat. §§ 75-1.1 *et seq.* ("NC UDTPA")
(On Behalf of Plaintiff Blake and the North Carolina Subclass)

105. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

106. Plaintiff Blake brings this claim on behalf of himself and the North Carolina Subclass.

107. N.C. Gen. Stat. § 75-1.1(a) states: "Unfair methods of competition in or affecting commerce, and unfair or deceptive acts or practices in or affecting commerce, are declared unlawful."

108. Defendant's failure to disclose that its data privacy measures are inadequate to protect Class Member Personal Information, and its continued use and support of the FTA platform with file transfer clients—who entrusted Accellion with Class Members' sensitive Personal Information—despite knowing that the FTA was unsecure and vulnerable to exploitation and data breaches, constitutes an unfair practice in violation of N.C. Gen. Stat. Ann. § 75-1.1.

109. Plaintiff Blake and North Carolina Subclass members are persons who provided their Personal Information to Accellion's clients, like Kroger, who in turn entrusted that sensitive information to Accellion in connection with file transfer activities.

110. Accellion knew for years that its FTA was unsecure, including at the time Plaintiff Blake and North Carolina Subclass members' Personal Information was entrusted to Accellion. In fact, Accellion had been encouraging file transfer clients for years to switch to its more secure product, Kiteworks.

111. Accellion's continued use and refusal to end support for the FTA in the face of a real security threat and risk of a data breach, all of which was reasonably foreseeable, constitutes unfair practices in violation of the NC UDTPA.

112. Accellion's practices offend public policy, are immoral, unethical, oppressive, and unscrupulous, and caused substantial injury to consumers.

113. Accellion's unfair acts or practices were the foreseeable and actual cause of Plaintiff Blake's and North Carolina Subclass members suffering actual damages.

114. Plaintiff Blake and North Carolina Subclass members suffered ascertainable loss as a direct and proximate result of Accellion's unfair acts or practices. Among other injuries, Plaintiff Blake and North Carolina Subclass members lost time and the privacy and value of their Personal Information.

115. Accellion's violations of the NC UDTPA present a continuing risk to Plaintiff and North Carolina Subclass members, as well as to the general public. Accellion's unlawful acts and practices adversely affect the public interest.

COUNT V
Violations of the Washington Consumer Protection Act
Wash. Rev. Code § 19.86.010, *et seq.* ("WCPA")
(On Behalf of Plaintiff Fehlen and the Washington Subclass)

116. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

117. Plaintiff Fehlen brings this claim on behalf of himself and the Washington Subclass.

118. Accellion, Plaintiff Fehlen, and Washington Subclass members are "persons" under Wash. Rev. Code § 19.86.010(1).

119. Accellion's acts or practices, as set forth above, occurred in the conduct of "trade" or "commerce" within the meaning of Wash. Rev. Code § 19.86.010(2).

120. Washington law prohibits "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or practices." Wash. Rev. Code §§ 19.86.020.

121. Defendant's failure to disclose that its data privacy measures are inadequate to protect Class Member Personal Information, and its continued use and support of the FTA platform with file transfer clients—who entrusted Accellion with sensitive Personal Information—despite knowing that the FTA was unsecure and vulnerable to exploitation and data breaches, constitutes an unfair practice in violation of the WCPA.

122. Plaintiff Fehlen and Washington Subclass members are persons who provided their Personal Information to Accellion's clients, like Kroger, who in turn entrusted that sensitive information to Accellion in connection with file transfer activities.

123. Accellion knew for years that its FTA was unsecure, including at the time Plaintiff Fehlen and Washington Subclass members' Personal Information was entrusted to Accellion. In fact, Accellion had been encouraging file transfer clients for years to switch to its more secure product, Kiteworks.

124. Accellion's continued use and refusal to end support for the FTA in the face of a real security threat and risk of a data breach, all of which was reasonably foreseeable, constitutes unfair practices in violation of the WCPA.

125. Accellion's practices offend public policy, are immoral, unethical, oppressive, and unscrupulous, and caused substantial injury to consumers.

126. Accellion's unfair acts or practices were the foreseeable and actual cause of Plaintiff Fehlen and Washington Subclass members suffering actual damages.

127. Plaintiff Fehlen and Washington Subclass members suffered ascertainable loss as a direct and proximate result of Accellion's unfair acts or practices. Among other injuries, Plaintiff Fehlen and Washington Subclass members lost time and the privacy and value of their Personal Information.

128. Accellion's violations of the WCPA present a continuing risk to Plaintiff and Washington Subclass members, as well as to the general public. Accellion's unlawful acts and practices adversely affect the public interest.

129. Under Wash. Rev. Code § 19.86.090, Plaintiff Fehlen and the Washington Subclass seek an order enjoining Accellion's unfair acts or practices, providing for appropriate monetary relief, including trebled damages, and awarding reasonable attorneys' fees and costs.

130. In accordance with Wash. Rev. Code § 19.86.095, a copy of this First Amended Class Action Complaint will be served on the Attorney General of Washington.

COUNT VI
Declaratory Relief
28 U.S.C. § 2201
(On Behalf of Plaintiffs and the Nationwide Class)

131. Plaintiffs reallege and incorporate all previous allegations as though fully set forth herein.

132. An actual controversy has arisen and exists between Plaintiffs and members of the Classes, on the one hand, and Defendant, on the other hand, concerning the Data Breach and Defendant's failure to protect Plaintiffs' and Class Members' Personal Information, including with respect to the issue of whether Defendants took adequate measures to protect that information. Plaintiffs and Class Members are entitled to judicial determination as to whether Defendant has performed and is adhering to all data privacy obligations as required by law or otherwise to protect Plaintiffs' and Class Members' Personal Information from unauthorized access, disclosure, and use.

133. A judicial determination of the rights and responsibilities of the parties regarding Defendant's privacy policies and whether they failed to adequately protect Personal Information is necessary and appropriate to determine with certainty the rights of Plaintiffs and the Class Members, and

so that there is clarity between the parties as to Defendant's data security obligations with respect to Personal Information going forward, in view of Accellion's continued custody of Personal Information.

PRAYER FOR RELIEF

Plaintiffs, individually and on behalf of the Class, by and through undersigned counsel, respectfully requests that the Court grant the following relief:

A. Certify this case as a class action pursuant to Fed. R. Civ. P. 23, and appoint Plaintiffs as class representative and undersigned counsel as class counsel;

B. Award Plaintiffs and Class Members actual and statutory damages, punitive damages, and monetary damages to the maximum extent allowable;

C. Award declaratory and injunctive relief as permitted by law or equity to assure that Class Members have an effective remedy, including enjoining Defendant from continuing the unlawful practices as set forth above;

D. Award Plaintiffs and Class Members pre-judgment and post-judgment interest to the maximum extent allowable;

E. Award Plaintiffs and Class Members reasonable attorneys' fees, costs, and expenses, as allowable; and

F. Award Plaintiffs and Class Members such other favorable relief as allowable under law or at equity.

JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

Dated: July 23, 2021

Respectfully submitted,

/s/ Tina Wolfson

TINA WOLFSON (SBN 174806)
twolfson@ahdootwolfson.com
ROBERT AHDOOT (SBN 172098)
rahdoot@ahdootwolfson.com
THEODORE MAYA (SBN 223242)
tmaya@ahdootwolfson.com
AHDOOT & WOLFSON, PC
2600 W. Olive Avenue, Suite 500
Burbank, CA 91505-4521

Telephone: 310.474.9111
Facsimile: 310.474.8585

ANDREW W. FERICH (*pro hac vice*)
aferich@ahdootwolfson.com
AHDOOT & WOLFSON, PC
201 King of Prussia Road, Suite 650
Radnor, PA 19087
Telephone: 310.474.9111
Facsimile: 310.474.8585

BEN BARNOW (*pro hac vice*)
b.barnow@barnowlaw.com
ANTHONY L. PARKHILL (*pro hac vice*)
aparkhill@barnowlaw.com
BARNOW AND ASSOCIATES, P.C.
205 West Randolph Street, Suite 1630
Chicago, IL 60602
Telephone: 312-621-2000
Facsimile: 312-641-5504

Attorneys for Plaintiffs and the Proposed Class